資料７－３

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

厚生労働省におけるサイバーセキュリティに関する取り組み

Ministry of Health, Labour and Welfare of Japan

令和６年度版 医療機関等におけるサイバーセキュリティ対策チェックリスト

- 令和６年度版「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」（令和６年５月13日付け医政参発0513・第6号医政局特定医薬品開発支援・医療情報担当参事官通知）を発出した。
  https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html
- 令和５年度版チェックリストの一部項目について、令和６年度に確認するものを参考項目として位置づけていたが、令和６年度において、すべての項目を確認することとした。

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）
医療情報システムの有無	医療情報システムを導入、運用している。（「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ（ / ）

○ 令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*１回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）1回目	目標日	2回目
1 体制構築	（1） 医療情報システム安全管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
2 医療情報システムの管理・運用	医療情報システム全般について、以下を実施している。			
	（1） サーバ、端末PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（2） リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（3） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	サーバについて、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（6） アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	ネットワーク機器について、以下を実施している。			
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（8） 接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
3 インシデント発生に備えた対応	（1） インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ（ / ）		

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
- 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

○ 参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付）1回目	目標日	2回目
2 医療情報システムの管理・運用	サーバについて、以下を実施している。			
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	端末PCについて、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
3 インシデント発生に備えた対応	（2） インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（3） サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。

令和５年度版

令和6年度版
医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。（「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ（ / ）	

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付）1回目	目標日	2回目	備考	R5年度項目
1 体制構築	医療情報システム安全管理責任者を設置している。(1-(1))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
2 医療情報システムの管理・運用	医療情報システム全般について、以下を実施している。					
	サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-(1))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-(2)) ※事業者と契約していない場合には、記入不要	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-(3)) ※事業者と契約していない場合には、記入不要	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	サーバについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	アクセスログを管理している。(2-(6))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7)	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		
	端末PCについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		
	ネットワーク機器について、以下を実施している。					
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
3 インシデント発生に備えた対応	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-(1))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-(2))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		
	サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-(3))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。
- R5年度項目欄（※）：「医療機関におけるサイバーセキュリティ対策チェックリスト（令和５年６月版）」において令和５年度中に対応することを目標として掲げた項目

令和６年度版

※チェック項目「サイバー攻撃を想定した事業継続計画（BCP）を策定している。」については、BCP 策定に関する手引きを別途お示しする予定。
※事業者確認用についても同様に改定を行った。

医療機関におけるサイバーセキュリティ確保事業

令和５年度第一次補正予算額　36億円

- 厚労科研*にて以下の課題が挙げられた。

①情報資産台帳等で把握されていない情報機器及び外部接続部が存在

・検査機器毎の保守回線等、外部接続部が多数あるケースがあり、医療機関ごとの状況は様々。（一医療機関あたり：７～47カ所）
・多くの院内ネットワークが異なったベンダーにより形成されており全体図を俯瞰的に把握できていない。
・ネットワークセキュリティのための必要最低限の設定がなされていない。

②バックアップ接続時の設定が適切になされていない。

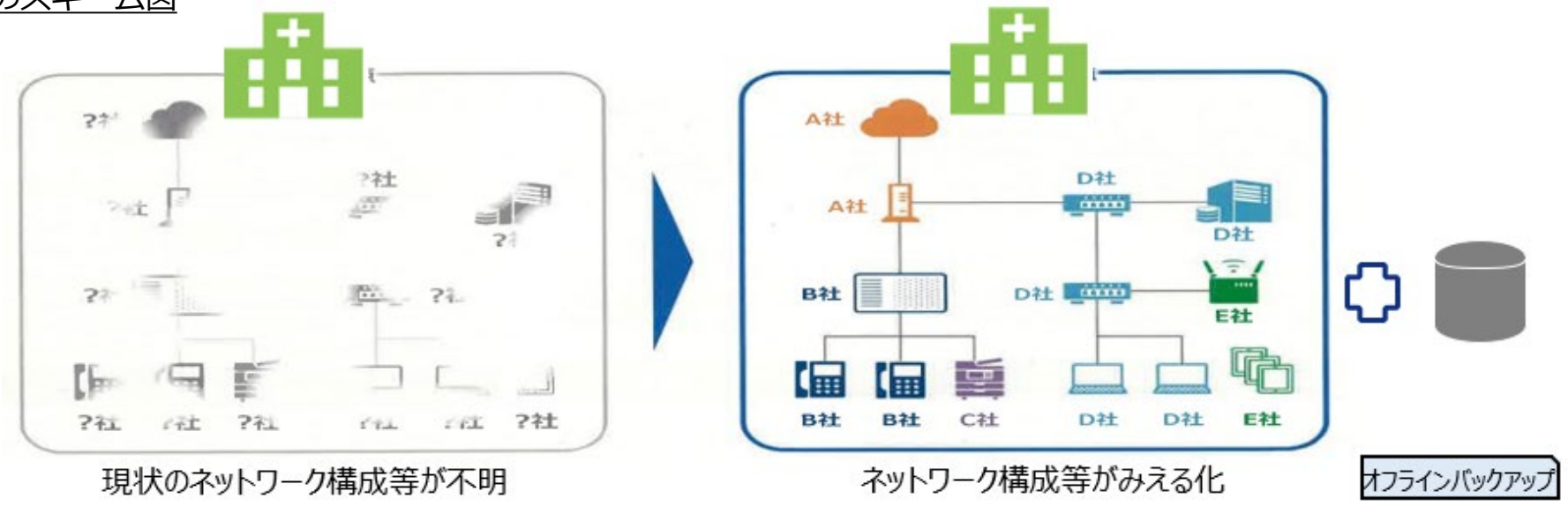
・ネットワークセキュリティのための必要最低限の設定がなされていない。

*厚生労働科学研究費補助金「医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究（令和3-4年度, 研究代表者：近藤博史）」

①　施策の概要

- 本事業は、医療機関におけるサイバーセキュリティの更なる確保のため、①外部ネットワークとの接続の安全性の検証・検査、②オフライン・バックアップ体制の整備を支援する。

②　施策のスキーム図



調査期間：2024年6月～2025年1月対象病院：2，002施設